Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices

Margit C. Scholl, Frauke Fuhrmann, L. Robin Scholl

January 2018

WILDAU

margit.scholl@th-wildau.de
http://www.th-wildau.de/scholl

LAND BRANDENBURG

wille@twz-ev.de
http://www.twz-ev.org/

Limitation of our research

- We reviewed publications of leading **academic journals** over the past decade
  in the field of **information security (IS)** and the **“human factor”,**
  influencing **factors** and **antecedents**,
  of information security **awareness** (ISA) and
  of information security awareness **trainings** (ISAT).

- From about 150 papers, 30 papers were not relevant for our research, so all in all our research bases on round about **120 scientific papers**.

- **Limits**: Much of the research on ISA is about staff and students at the university level, with a certain amount focusing on company employees. **There are few e-government studies, although public administrations have electronically processed sensitive and critical information for decades**. In order to overcome this limitation, we are particularly keen to stimulate projects in this area. More research in the nonlinear and complex field of ISA and ISAT is necessary.

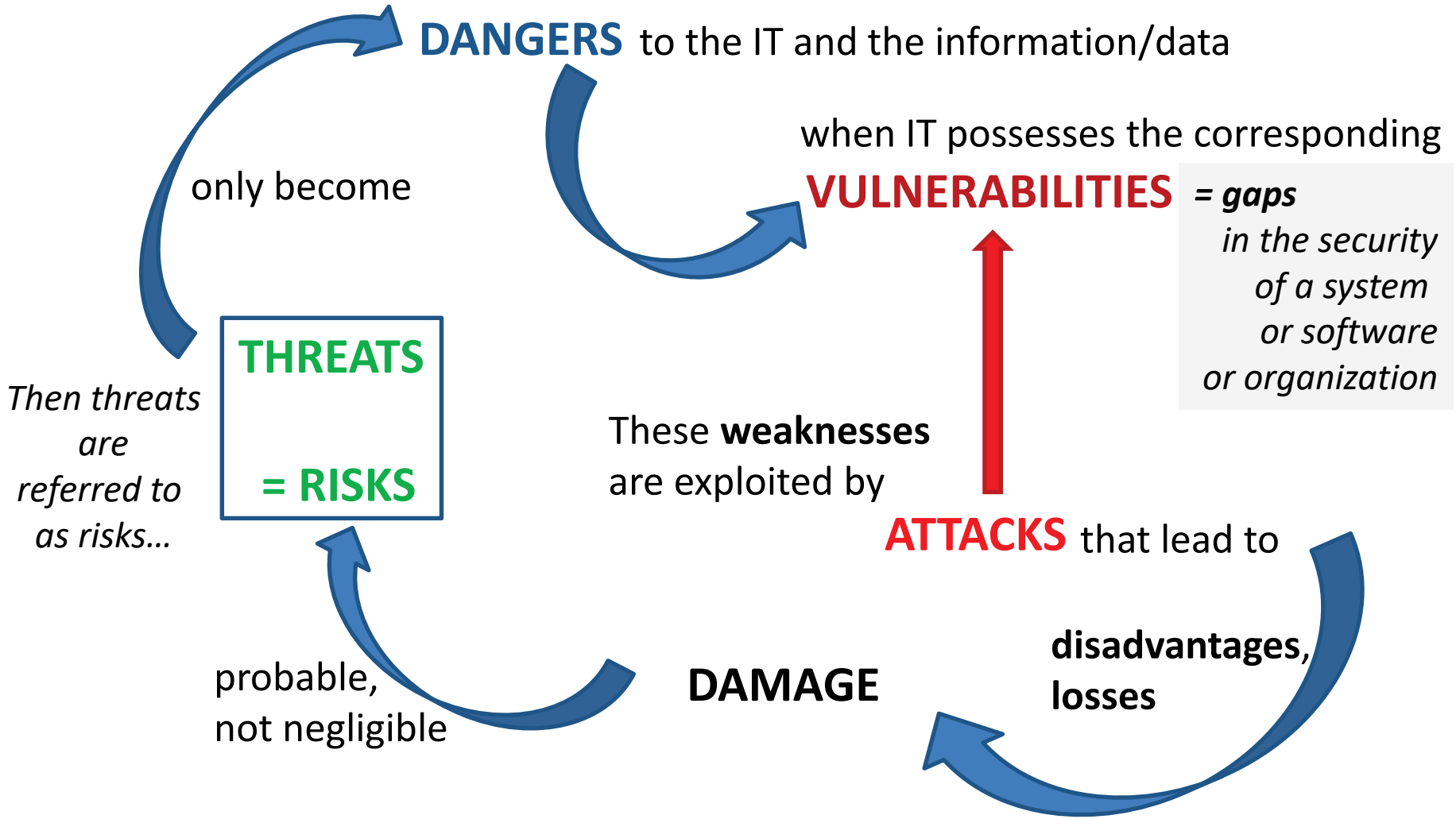
Information security (IS) – Why?

- **Dependence on the ICT**
  + modern information society
    + computer networks
      + more and more important to (business) processes

- **Digitization**
  + technological, business, economic, organizational developments
    + opens the door into a comprehensively networked society
      + networked administration (smart government)
        further reduces bureaucratic burdens

ICT / digitization transmits, processes, and stores large amounts of *sensitive* data and a *wide variety* of information.

Vulnerabilities, threats and risks



Digitization and consequences …

spam

e-mail attacks + 29%

https://www.proofpoint.com/de. Accessed: 28.11.2017.

64% ransomware

malware

24% banking trojans

virus

worms

adware

scareware

hoax

spyware

fake

CEO fraud

backdoor

SQL-injection

+ 85%

botnet armies

rootkit

oder local file inclusion

keylogger

DDoS + 8 %

prejudicial URLs + 600%

APT

web attacks + 30%

phishing links + 10%

zero day exploit

identity theft

doppelganger

drive by exploit

social engineering

domains 20:1

fake customer service accounts + 5%

Picture: A Tale, https://de.toonpool.com/cartoons/Wahl%20in%20Frankreich_291937. Accessed: 28.11.2017.

Threats 3/2017

Why?

Summary of all reports:

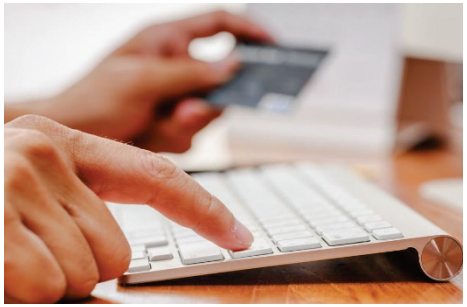
Cyber attacks target people, not technologies!

https://www.proofpoint.com/de.
Accessed: 28.11.2017.

Research findings I

- Internet and web-based systems have been introduced for millions of customers **without adequate information security (IS)**.
- One direct result was that criminals shifted their attention to the end user under their new motto:

“ Do not try to hack into the company’s IT systems; it may be very difficult—go for the naïve end user!” [74].



Picture: https://static.giga.de/wp-content/uploads/2016/07/Windows-10-Kosten-rcm992x0.jpg. Accessed: 28.11.2017.

Human being as a „risk factor“?

Ponemon INSTITUTE

The Need for a New IT Security Architecture: Global Study

Sponsored by Citrix

Independently conducted by Ponemon Institute LLC

Publication Date: January 2017

The **51- to 69-year-olds** are in particular easy to trick.

The group of **35 to 50** is most likely to settle over known rules.

The most risky group are the young employees, the group of the Millennials (**18 to 35**) because they use all sorts of unauthorized technology.

Strategic deficits ...

Not even half of the (surveyed) companies in Germany are sufficiently prepared for a cyberattack.
Digitalverband Bitkom 09/2017

Managers pay ransom rather than to invest in new protection features —big risk, because ransom payments usually are six-figure amounts.
Verizon's Data Breach Investigations Report 2017

74% of the security incidents stay over more than six months undetected.
Ponemon Institute Report

Less than 50 % of organizations have an IT security and training program for employees
Verton, NY, 2002.

Only four out of ten companies have an emergency / continuity management (43%).
Digitalverband Bitkom 09/2017

Only 63 % of respondents take measures to raise awareness for information security and 40.5 % of these organizations do not measure the effectiveness of their training.
Allianz für Cyber-Sicherheit, 2015

46% of all companies believe that they have—regarding their cybersecurity skills—a critical shortage.
Enterprise Strategy Group Brief, February 2016

Research findings II

- If a single user action can compromise an entire security program, **the problem is the security program itself** [76].

- The safety behavior is strongly influenced by the **personal risk perception of the employees** and these perceptions can be positively changed [6] (by awareness raising and training).

Research findings III

- The **top management** must play a ***proactive*** role in shaping employees' compliance with IS behavior.

- The **integration of formal and informal mechanisms** can enhance the **interaction** between employees.

RQ#1

- **RQ#1:**

  What ***is*** ISA (information security awareness) actually?

  What **factors** are used in the scientific literature to define it?

  How can the correlation to an organizational **IS culture** be interpreted and rules for livable security created?

RQ#1: ISA

- There is no uniform and binding definition of ISA.
- Many scientific articles based on the **KAB** model: *knowledge, attitude and behavior.*
- Scholars show that knowledge/education about the IS of users is a basis for reflecting on their own attitudes.
- The overall goal of most literature in this context is a **better understanding** of people's behavior as a means to develop it in the proper way.

RQ#1: Factors

- There is **no simple linear cause-and-effect relationship** between knowledge and attitudes,
- and certainly not with regard to the ***real* IS behavior** of people.

- **Psychological** factors, subjective norms, and the sociocultural, gender and age background in **nonlinear and complex interactions** have a major influence on human ISA and IS behavior.

  (user-centered approach)

- A main problem for human beings seems to be the **application** of IS knowledge **in *real-world* situations**.

RQ#2

- **RQ#2:**

  What are the dependencies/connections/ correlations between these factors and the ISA **in practice**?

  What are the **consequences** for individual and organizational learning processes in the area of IS?

RQ#2: Practice

- The **improvement of perception and comprehension** can advance a person's ability to project **real-life situations**.

- And it seems that the **constructs of organizational impact and attacker assessment** have a stronger influence on the ISA than technical knowledge.

- **Management and employees have to learn their pivotal role** for the IS of an organization.

RQ#2: Learning processes

- The learning process in organizations must be based on the **user-centered approach**.
- The user-centered approach pays attention to **target groups**, gender, and culture, which is based on individual knowledge and skills as well as on **concrete work connections**.
- The user-centered approach should also enable **exchange**.
- The **integration of formal and informal mechanisms** can enhance the interaction between employees.

RQ#2: Learning processes

- Frequent interaction is the basis for the formation of **inter-personal relationships and psychological attachment** to the organization.

- **Threat analysis, self-efficacy, and response effectiveness** have a significant impact on the intention to comply with the IS guidelines

- Therefore, such **aspects of emotionalization and motivation** should be incorporated into the sensitization to and training of ISA.

RQ#3

- **RQ#3:**

  What and how is ISA **measured**?

  How is ISA **related** to IS compliance?

RQ#3: Measurement

- We found that **only a few organizations use different metrics** for a deeper and continuous measurement of their awareness program [58].

- **ISAT should be ongoing** as the organization changes and employees move into and across roles, with a **focus** on what is necessary for their jobs [39].

- Therefore, **ISAT should not overwhelm employees** with information or take up excessive paid work time [72].

- Rather than relying on generalized computer-based packages, IS training should be geared to the **specific work environment**.

Training and raising awareness

- **Understanding and accepting safeguards:** Technical security safeguards often lead to less user-friendly IT.

User will only accept such safeguards, when they understand why the restrictions, for example for surfing, for sending and receiving e-mail, or for password usage, are necessary.

- Employees are only able to actually follow the security policies decided upon when thy know how to handle the IT securely and confidently.

Spiral of transformative interaction

ISA is necessary for a successful digitization that

… requires

a strategy,

… guarantee

an appropriate IT security level,

… needs

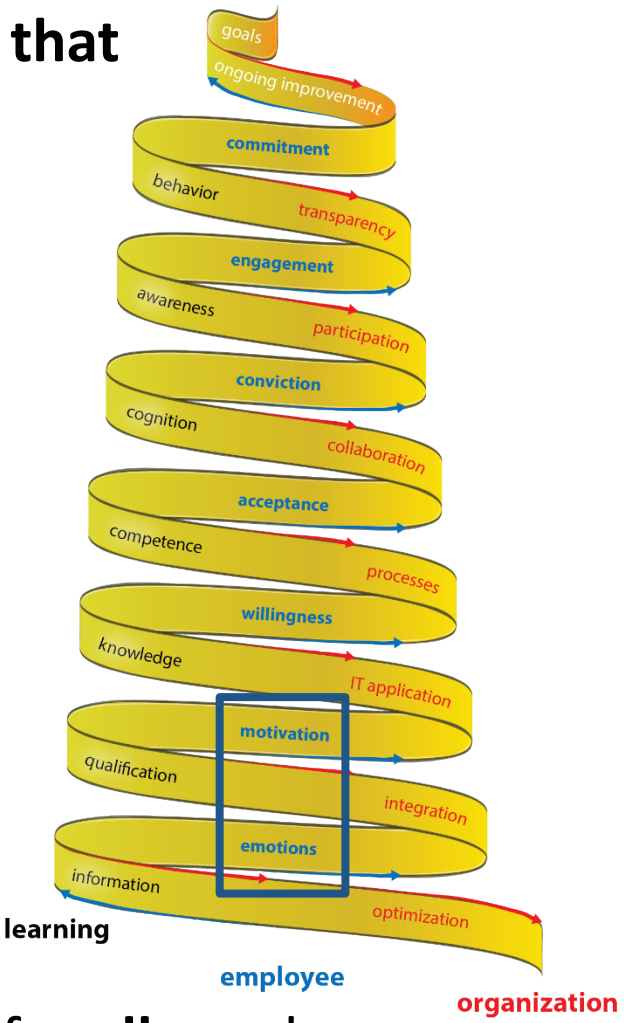
sufficiently qualified personnel,

… demands

a cultural change in the organization,

… needs

a continuous, target group oriented training for **all** employees



RQ#3: Compliance

- There are many **sanctions** in dealing with disregard of rules, but employees **will not be rewarded** if they comply with the IS security policy [14].

- Organizations are aware that this **'comply or die' approach does not work** for modern enterprises where employees collaborate, share, and show initiative.
  However, **they do not have an alternative approach** to fostering secure behavior [38].

- **Countermeasure awareness** was shown to be a **significant indicator** of perceived need for digital IS [34].

RQ#3: Compliance

- It seems that **attitudes toward compliance** with IS organizational policies also have a significant effect on the **behavioral intention** regarding IS compliance, whereby **policies must be livable** [31].

- The top management must be a **role model** and **give advice**, that should be seen as an enabler that supports the organization's goals.

- Creating an **effective ISA program** requires **targeted communication** and training that caters to **specific** employee groups.

RQ#3: Compliance & culture

- **ISA processes** are associated with **interrelated changes** that occur at the **organizational**, the **technological**, and the **individual level** [71].

- As a result of this [61],
  an organization needs to roll out **a series of ISA programs** oriented toward **perception, comprehension, and projection**.

  (real-life situations)

RQ#4

- **RQ#4:**

  How can ISA trainings (**ISAT**) **be designed** in practice to be efficient, effective, and sustainable?

  What **methods** are relevant from a scientific point of view?

RQ#4: ISAT

- Although scientific research indicates a general need for (cyberthreat) education, trainings, and awareness [35, 37, 45, 61]

  our review of the scientific literature shows that **the *design* of the ISA trainings has not been the subject of significant research.**

- Only a few studies from the literary field *knowledge, attitude, behavior* give (only general) recommendations for the design of training measures [50, 64].

- **“Awareness campaigns should be tailored to employees’ needs”** [6].

Security policies bring restrictions ...

Picture: Paolo Calleri, https://de.toonpool.com/cartoons/Weihnachten%202016_283863. Accessed: 28.11.2017.

RQ#4: ISAT

Why have mainstream ISA techniques failed?

- A **"technocratic" view** of risk communication [65]—criticized by experts in safety risk communications as ineffective and inefficient.

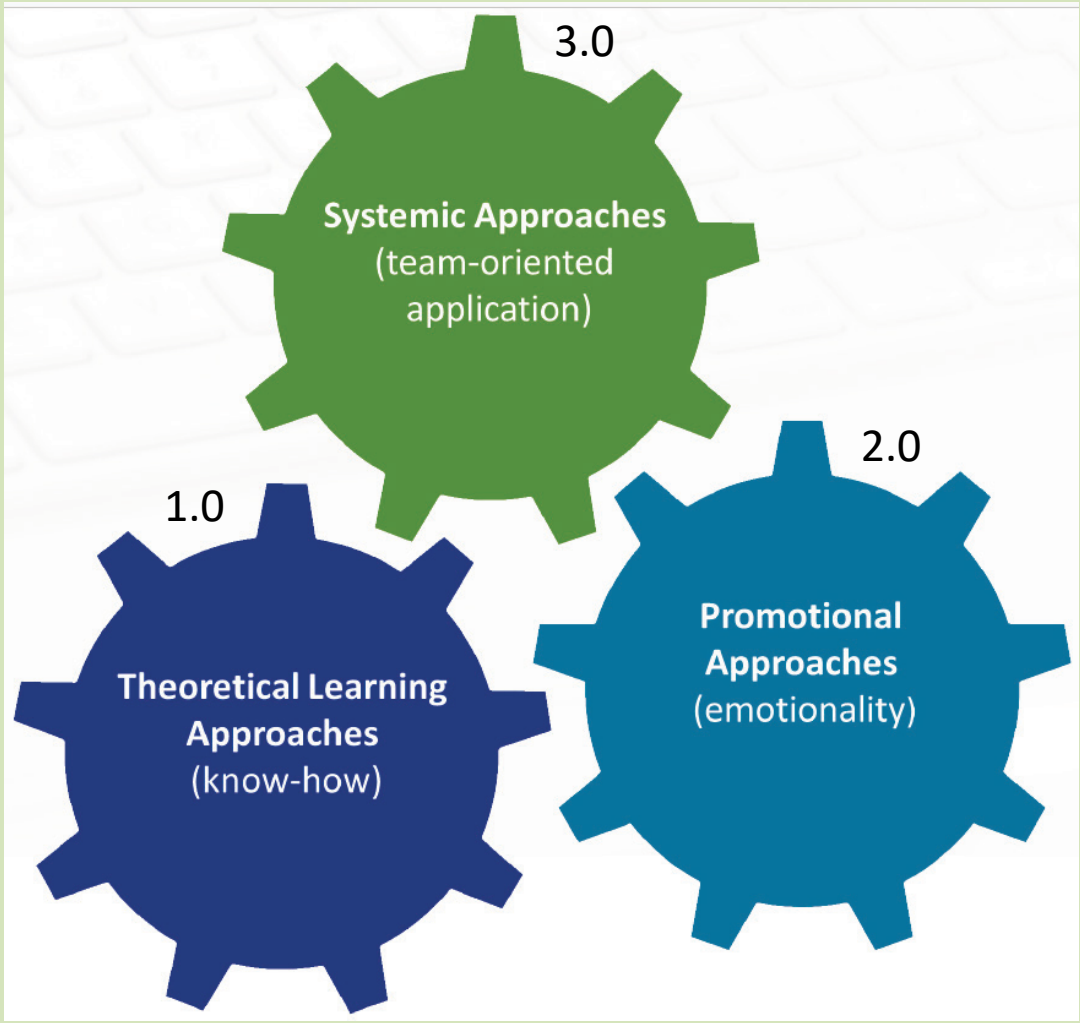
- Ignorance of the daily mix and **overlap between work and home**.
  "If you don't change home security behavior, it is hugely more difficult to effect change in the office" [13].

Why have mainstream ISA techniques failed?

- **Policies** "ending up as **long lists of dos and don'ts**"— most employees only access them as a duty, „which has little to no effect on their security behavior" [38].

- A training with the hope of addressing security awareness gaps **cannot** be sufficient to ensure **compliance with security culture** [24].

Sensitization through ISAT 3.0



RQ#4: ISAT consequences

Goals of awareness-raising

- Increasing the level of awareness of the employees for information security is intended to do the following:
  - Help them understand why security is important
  - Increase awareness that it is every employee's duty to conscientiously implement the security safeguards
  - Ensure each employee feels more responsible for security
  - Improve their knowledge of information security
  - Promote the early detection of security-related incidents
- **Be target group orientated!**

RQ#4: ISAT consequences

- The **emotional level** should be explicitly addressed, because social participation in a communicative team process is a key component in awareness-raising activities based on **psychological** theories [60].

- Learners must **directly see/feel the consequences** of their actions and should get a sense of their knowledge level in dialogue.

- Game-based learning (GBL) is especially effective as a means **to stimulate motivation and change behavior** and should be explicitly used for **raising awareness**.

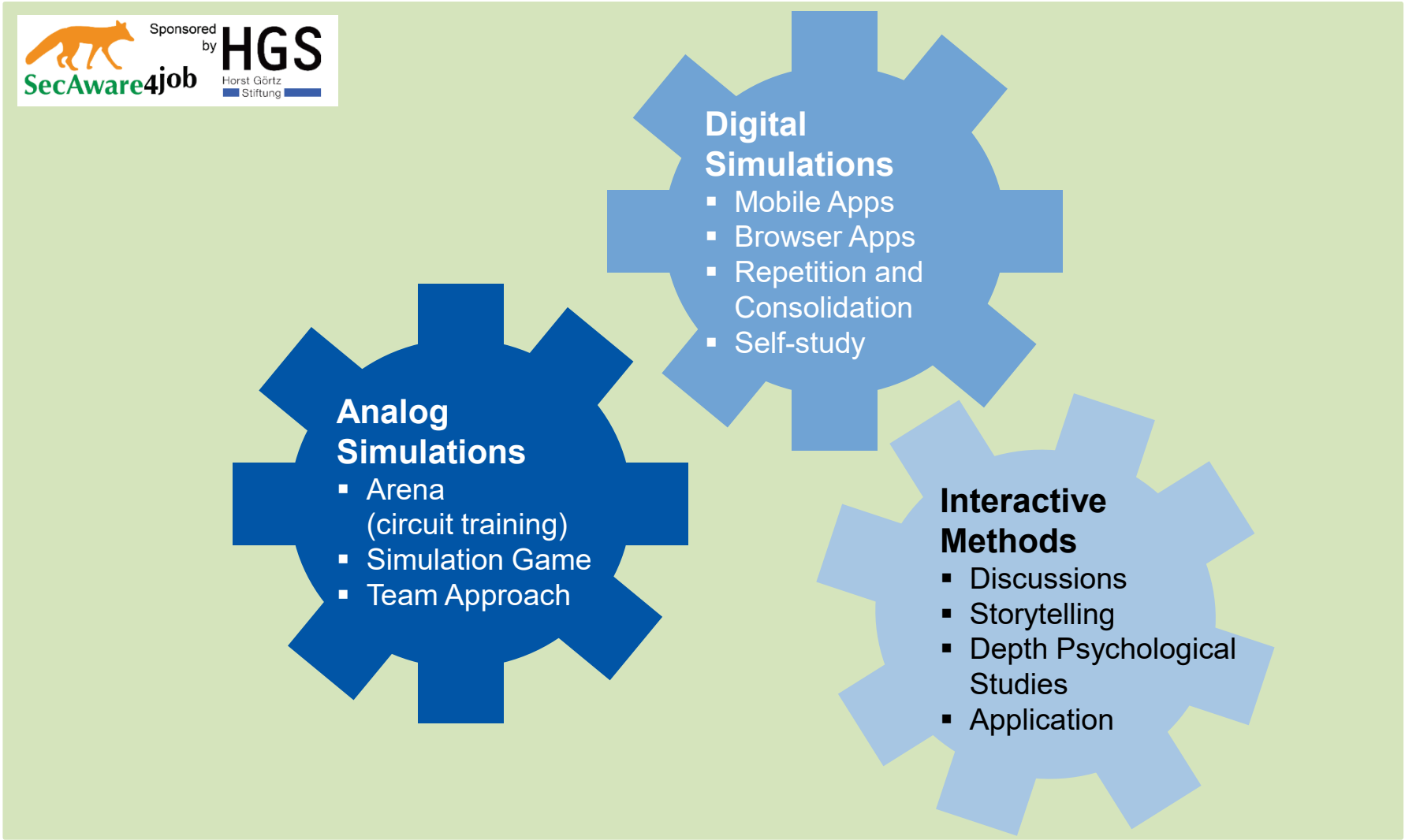
Why?

Our life is analogue … even in times of digitization …

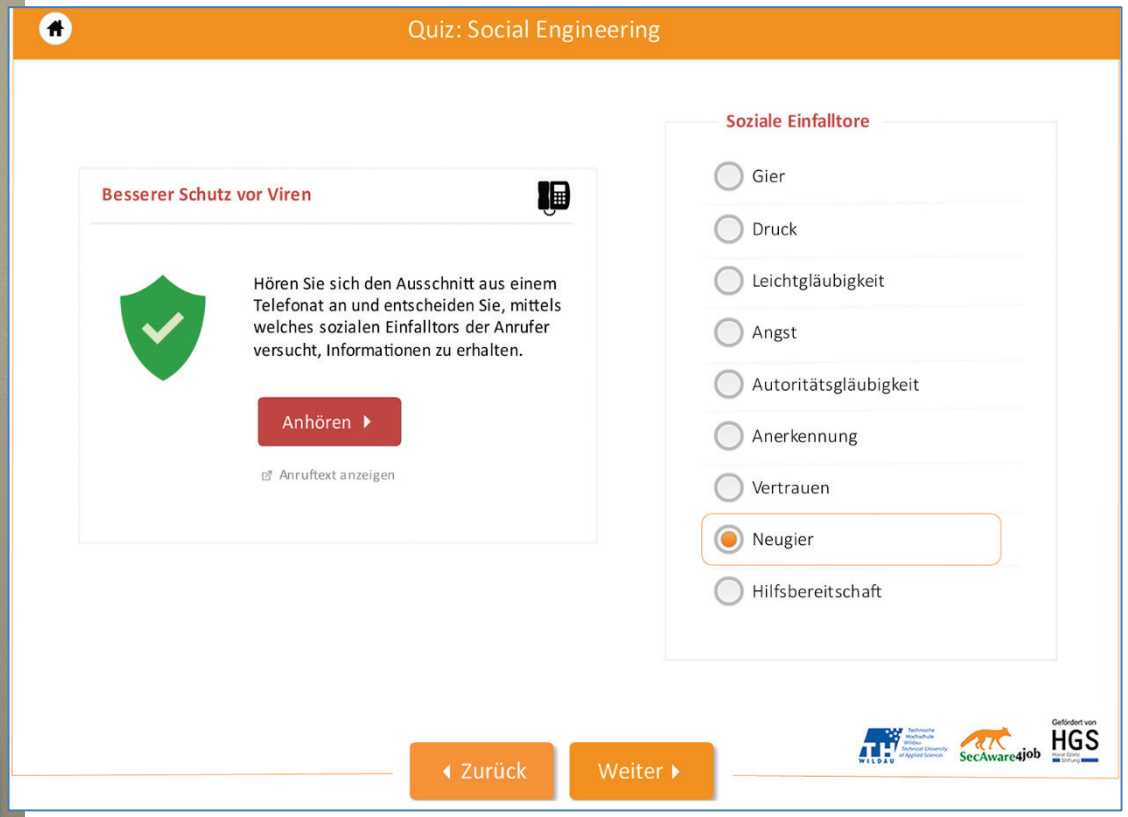
Why?

Picture: Jan Tomaschoff, https://de.toonpool.com/cartoons/Technik_303843. Accessed: 28.11.2017.

ISAT methods: Sensitization through GBL



ISAT methods: analogue and digital GBL



Social Engineering

ISAT methods: analogue/digital GBL and team

Interactive Methods

with discussions, experiences and expectations, and storytelling

Conclusion and Outlook

- Despite the increasing interest of researchers on the topic **awareness remains a critical issue of IS** [69].
- To protect the organizational assets, including user information and systems, **the human side of security should also be managed** [37] [67] [77] and **plays a significant role** in the successful delivery of IS in today's organizations [6].
- Moreover**, a clear set of IS principles needs to be identified and communicated** [38].
- Learning through integrating **target-orintated, interactiv analog, digital *and* team-orientied** methods as an **ongoing process**.

Human being—„Critical factor?“

A lack of understanding of security issues coupled
with the pervasive use of computers…

Knowledgeable human beings are better at preventing modern IS breaches…

They can efficiently and effectively respond to incidents by reporting them promptly…

Technology solutions alone are not sufficient to ensure IS countermeasures!

Previous IT security mechanisms have reached their limits.
IS is about more than technology.
Information systems involve human beings, and users do not always act the way they are supposed to.

Summary

Technical security alone is **not enough**.

Lack of sensitivity **is** still in business.

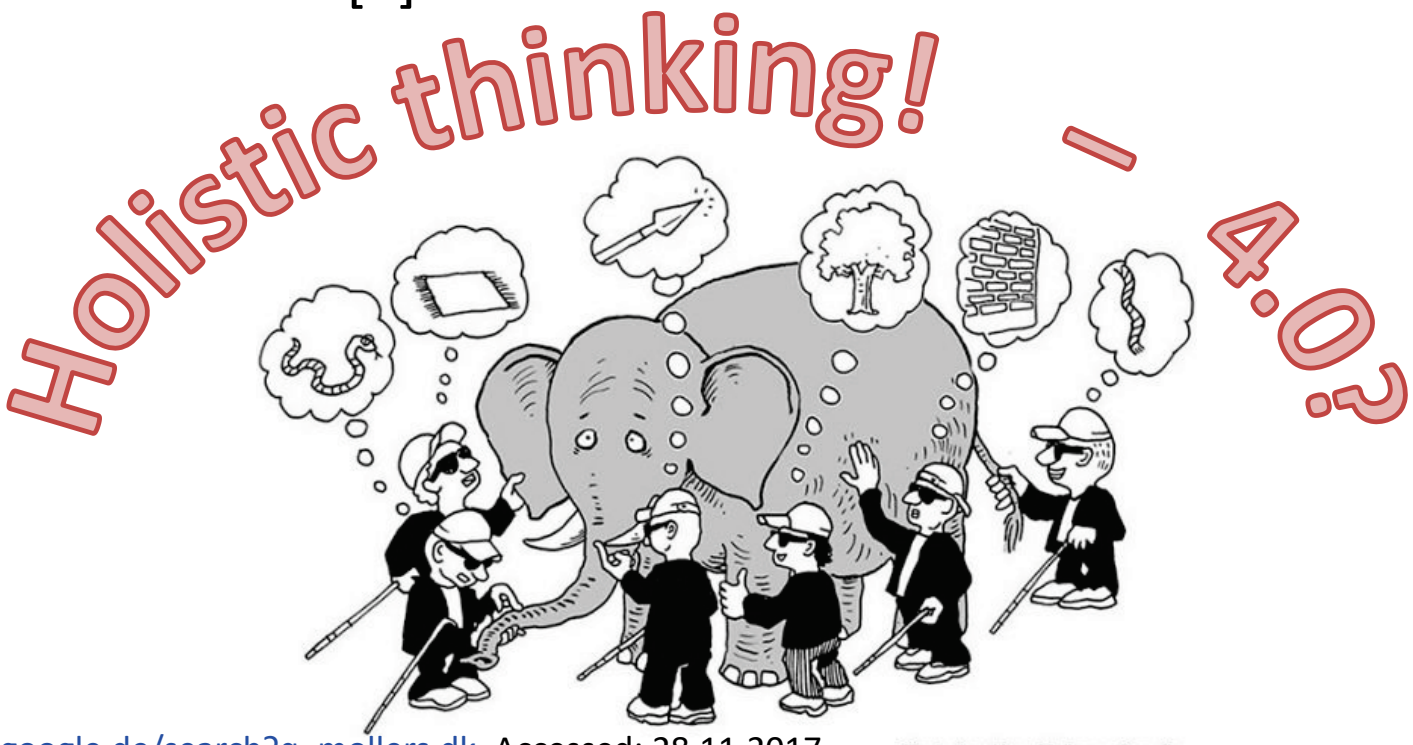
Security behavior is necessary for **all** employees in the workplace.

Predefined regulations have **to be lived**.

Regulations can be more easily complied with, the more **informed** the employees are about the facts and the better human being **understand** the reasons for them.

The Six Blind Men …

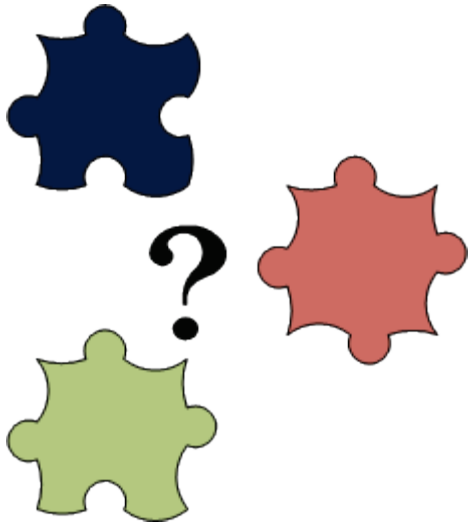
In a general way, ISA programs may generate a false sense of security, as taking part in ISA programs reduces perceptions of vulnerability, while the intentions for compliant security behavior are not affected [4].



Picture: https://www.google.de/search?q=mollers.dk. Accessed: 28.11.2017.

Questions & Comments

Thank you for your attention!



margit.scholl@th-wildau.de

www.th-wildau.de/scholl

http://secaware4job.wildau.biz